Claims:

(1)
(Gen. [illegible])

1) Division

(2)? (3)

In any circuit or computer program for computing reciprocals in a mathematical system such as a finite field or ring or modular arithmetic system,

(4)
What are the steps sequence

?

5 where the reciprocal is built up as a linear combination 6 of two or more working variables or registers that are (5) initialized at the start of the computation,

and where the building up is a sequence of operations chosen from

(6 shifting a variable,
adding one variable to another,
subtracting one variable from another,
negating a variable,
adding or subtracting a multiple of one variable to or from another,
exchanging variables,
permuting variables,
(8 or renaming variables;

? (8) ? (8)

X I claim the corresponding method or circuit for computing a quotient of two quantities, a numerator and a denominator, by [illegible] (3) initiali~~zing said wor~~king variables or registers, at the start of the computation, to different values, specifically, each working variable or register is initialized to a value equal to the product of the numerator times the corresponding initial value from the reciprocal circuit or program.

2) Quadratic Equations.

I claim any circuit or computer program which solves quadratic equations in a finite field or ring of characteristic 2 of even degree, by adding, subtracting, or xoring selected values from a table, with the selection being determined by examining the coefficients and parameters of the quadratic equation, and quantities derived from the coefficients and parameters, said values being combined together with partial solutions determined by directly examining the coefficients and parameters of the equation and quantities derived from the coefficients and parameters.

3) I claim any method of solving a quadratic equation in a characteristic 2 field or ring that computes some of the solution bits in a first phase, and then fills in the rest of the solution bits in subsequent phases.